１ － １

平成 28 年度
情報セキュリティに係る監査報告書
（公開用）

平成 28 年 12 月

総務部情報管理課情報管理班

第１章　実施概要

１．目的

本監査は、特定個人情報等の重要情報資産の取扱いを委託している「株式会社ディー・エス・ケイ」において、情報セキュリティが適切に実施されているかを点検することを目的とする。

２．監査対象

株式会社ディー・エス・ケイ柏事業所

３．監査対象期間

平成 28 年 9 月 15 日～平成 28 年 11 月 9 日

４．監査実施者

印西市総務部情報管理課情報管理班
板倉　主査
秋山　主査

５．実施方法

（１）予備調査

株式会社ディー・エス・ケイに対し、セキュリティに関する項目等について照会を行った。(別紙)

（２）実地調査

平成 28 年 11 月 9 日、株式会社ディー・エス・ケイ柏事業所を訪問し、情報資産の取扱いや情報セキュリティにかかわる項目について、資料閲覧、ヒアリング、実態確認を行った。

６．参考基準

点検項目については「地方公共団体における情報セキュリティ監査に関するガイドライン」（総務省　平成 27 年 3 月分）に準拠している。

第２章　監査結果

１．監査結果

株式会社ディー・エス・ケイについては、ＩＳＭＳおよびプライバシーマークの認定を受けており、同認定を受けるためには、対策基準などの文書の策定や、カードの管理などセキュリティ面での安全性の調査が行われているものである。

今回の監査においても、情報セキュリティの観点から対策が適切に管理されていると判断した。

２．改善検討の余地

２点、改善検討の余地が見受けられた。

予備調査項目

別紙

			回答
基本項目	管理運営基本方針	管理運営基本方針を定め、文書化しているか	
	セキュリティ実施基準	セキュリティに関する実施基準を定め文書化しているか	
	障害等対策基準	障害等の発生時の対応にかかわる基準を定め文書化しているか	
	改定の手順	基準を改定する場合の手順が定められているか	
資産の管理	管理台帳	情報資産について、資産が分類され、重要な資産については管理台帳が作成され、定期的に見直されているか	
	適切な管理	情報資産の分類に従い、適切な管理がされているか	
	機器の取り付け	サーバ等の機器について、火災や振動などの影響を可能な限り排除された場所に設置されているか	
	運搬	機密性の高い情報資産を運搬する場合、管理者の許可を得た上で、必要に応じ鍵付きのケース等に格納し、暗号化又はパスワードの設定を行う等、情報資産の不正利用を防止するための措置がとられているか	
	盗難防止措置	情報資産の盗難防止措置の対策はとられているか	
サーバ	冗長化	サーバの冗長化がされているか	
	障害対策基準	サーバの障害対策基準が定められ文書化されているか	
	障害対応	サーバに障害が発生した場合、システムの運用停止時間を最小限にする対策が講じられているか	
機器	機器の電源対策基準	停電等に備えた予備電源の設置基準等が定められ文書化されているか	
	機器の電源対策	停電等に備えた予備電源が備え付けられ、定期的に点検されているか	
	機器の定期保守	サーバ等の機器の定期保守が実施されているか	
	機器の修理	電磁的記録媒体を外部の事業者に修理させる場合、情報が漏えいしない対策が講じられている	
	機器の廃棄等	廃棄又はリース返却する機器内部の記憶装置からすべての情報が消去され、復元が不能な状態になっているか	
通信回線	通信ケーブル等の配線	通信ケーブルや電源ケーブルの損傷等を防止するための対策が講じられてい	
	通信回線の管理基準	会社内の通信回線及び通信回線装置は管理基準に従って管理されているか	
	通信回線の選択	機密性の高い情報資産を取扱う情報システムに接続している通信回線は適切な回線が選択されているか	
管理区域	管理区域への入退室	管理区域への入退室が制限され管理されているか	
	管理区域への機器持込み	機密性の高い情報資産を扱うシステムを設置している管理区域に当該情報システムに関連しない機器等を持ち込ませていないか	
	管理区域への機器の搬出入	管理区域への機器の搬入出の際は職員を立ち会わせているか	
内部ネットワーク	ネットワークの接続制御	ネットワークに適切なアクセス制御が施されているか	
	ファイアウォール、ルータ等の設定	フィルタリング及びルーティングについて設定の不整合が発生しないように通信ソフトウェア等が設定されているか	
	無線LAN	無線LANを利用する場合には解読が困難な暗号化及び認証技術が使用されているか	
パスワード	入力	システムログイン時にパスワード入力するよう設定されているか	
	認証	重要な業務については、パスワード以外の認証を使用しているか	
	管理	パスワードは当該本人以外に知られないように取扱われているか	
	変更	パスワードは定期的に変更されているか	
	パスワードファイルの管理	パスワードの暗号化やオペレーティングシステム等のセキュリティ強化機能等でパスワードファイルが厳重に管理されているか	
アクセス制御	アクセス制御にかかわる基準	アクセス制御にかかわる基準が明文化されているか	
	利用者IDの取扱い	利用者IDの登録、変更等に係る手続が明文化されているか	
	利用者IDの登録・権限変更の申請	情報システムにアクセスする業務上の必要あるいは権限変更が生じた場合、申請を行っているか	
	利用者IDの抹消申請	アクセスする業務上の必要が無くなった場合は従業員から申請を行っているか	
	利用者IDの点検	必要のない利用者IDが登録されていないか	
	特権IDの取扱い	管理者権限等の特権を付与されたIDの取扱い手続が明文化されているか	
	外部からのアクセス	外部からのアクセスを許可している場合、手続が明文化されているか	
従業員	関係法令等の順守	個人情報の保護の順守などが規程等として文書化されているか	
	規程等の掲示	従業員等が常に最新の規程等を閲覧できるよう掲示されている	
	研修の実施	情報セキュリティ研修・訓練が定期的に行われているか	
	業務以外での使用の禁止	業務以外目的での情報資産の持出し、情報システムへのアクセス、電子メールアドレスの使用及びインターネットへのアクセスは行われていないか	
支給以外の端末等の業務利用	手順の文書化	支給以外の端末等の利用を許可している場合は、利用手順が文書化されてい	
	機密性の高い情報資産への情報処理作業	支給以外の端末等の利用を許可している場合は機密性の高い情報資産には支給以外の端末等による情報処理作業は行われていないか	
バックアップ	バックアップの実施	定期的なバックアップが実施され、媒体が適切に保存されているか。	
情報資産の持出し	外部持出し制限	従業員等がモバイル端末、電磁的記録媒体、情報資産及びソフトウェアを外部に持ち出す場合、許可を得ているか	
	持出し持込みの記録	端末等の持出し及び持込みの記録が作成され保管されているか	
	電子メール転送	権限のないものによる、外部から外部への電子メール転送が行えないようになっているか	
報告	情報セキュリティインシデントの報告手順	情報セキュリティインシデントを認知した場合の報告手順が定められ、文書化されているか	
	情報セキュリティインシデントの報告	情報セキュリティインシデントを認知した場合、手順に従って報告されているか	
記録	作業の記録	所管する情報システムの運用において実施した作業記録が作成されている	
	仕様書等の管理	情報システム関連文書は施錠したキャビネットやアクセス権を制限したフォルダで管理されているか	
	ログの管理	各種ログ及情報セキュリティの確保に必要な記録が取得されているか	
	障害記録	障害記録が保存されているか	
不正プログラム等の対策	ファイアウォール等の設置	Webサーバをインターネットに公開する場合、外部ネットワークとの境界にファイアウォール等が設置されているか	
	フリーメール	フリーメール、ネットワークストレージサービス等が使用されていないか	
	ソフトウェアの無断導入	許可なく業務用のパソコンやモバイル端末にソフトウェアが導入されていないか	
	不正コピーソフトウェアの利用禁止	不正にコピーされたソフトウェアが利用されていないか	
	ネットワーク接続の禁止	従業員等が私物のパソコンやモバイル端末をネットワークに接続していないか	
	機器の改造及び増設交換の申請	業務用のパソコンやモバイル端末の改造や増設交換を許可なく行っていないか	
	不正プログラムに感染した場合の対処	不正プログラムに感染した場合又は感染が疑われる場合、LANケーブルが即時取り外す等の対処を教育しているか	
外部委託事業者	外部委託事業者の検査	再委託先のセキュリティ検査を行っているか	